4121-37202 thru 4121-37214

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 July 2003 (17.07.2003)

PCT

(10) International Publication Number
WO 03/058457 A1

(51) International Patent Classification[7]: G06F 12/14, H04L 9/00

(21) International Application Number: PCT/US02/41819

(22) International Filing Date:
31 December 2002 (31.12.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/345,689 31 December 2001 (31.12.2001) US

(71) Applicant *(for all designated States except US)*: **CITADEL SECURITY SOFTWARE INC.** [US/US]; 8750 N. Central Expressway, Suite 100, Dallas, TX 75231 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **BANZHOF, Carl, E.** [US/US]; 4145 Goodfellow Dr., Dallas, TX 75229 (US).

(74) Agent: **CONLEY, ROSE & TAYON**; Suite 330, 5700 Granite Parkway, Plano, TX 75024 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

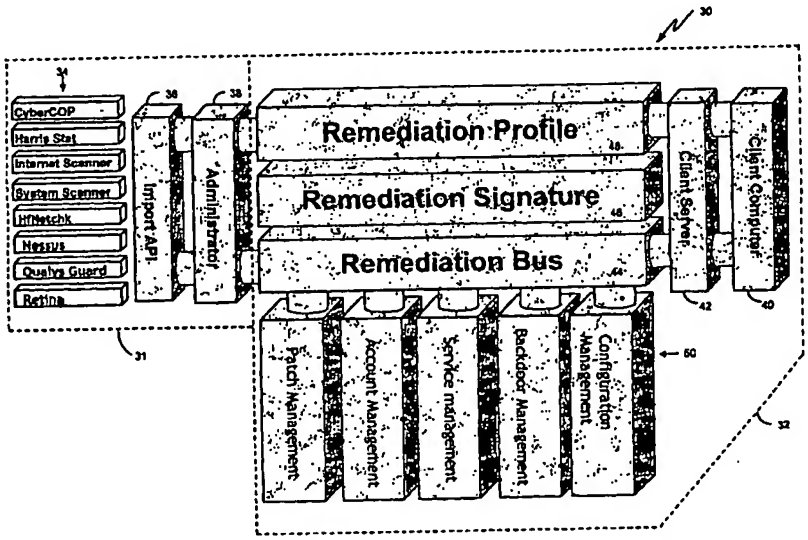
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA,*

[Continued on next page]

(54) Title: AUTOMATED COMPUTER VULNERABILITY RESOLUTION SYSTEM



(57) Abstract: A system and process for addressing computer security vulnerabilities. The system and process generally comprise aggregating vulnerability information on a plurality of computer vulnerabilities; constructing a remediation database of said plurality of computer vulnerabilities; constructing a remediation signature (46) to address the computer vulnerabilities; and deploying said remediation signature (46) to a client computer (40). The remediation signature (46) essentially comprises a sequence of actions to address a corresponding vulnerability. A managed automated approach to the process is contemplated in which the system is capable of selective deployment of remediation signatures (46); selective resolution of vulnerabilities; scheduled deployment of remediation signatures (46); and scheduled scanning of client computers (40) for vulnerabilities.

WO 03/058457 A1

CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations*

Published:

— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

AUTOMATED COMPUTER VULNERABILITY RESOLUTION SYSTEM

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims priority from U.S. Provisional Application serial no. 60/345,689 filed on December 31, 2001.

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

Not applicable.

REFERENCE TO A MICROFICHE APPENDIX

Not applicable.

FIELD OF THE INVENTION

[0001] The invention relates generally to a method and system for resolving security vulnerabilities in computers and, more particularly, to a vulnerability resolution system in which computer security vulnerability information from one or more sources can be aggregated and comprehensive remediation updates can be generated for managed automated distribution to target client computers.

BACKGROUND OF THE INVENTION

[0002] Computers, computer systems, and the applications running thereon are becoming increasingly complex. In addition, with the advent of the Internet and other modern networking technology, computers have become increasingly interconnected and remote accessibility of individual computers and computer networks has become more and more common. In part as a result of this complexity, the number of computer security vulnerabilities that need to be addressed continues to increase. For example, in the year 2000 alone, 650 operating system vulnerabilities were identified, including 126 in the Windows 2000/NT platform and another 46 in the Windows 9x platform. The Computer Security Institute reported 417 vulnerabilities for the year 1999, 1090 vulnerabilities for the year 2000, 2,437 in 2001, and a projected 4000+ vulnerabilities in 2002. Given these trends, it has become increasingly difficult to protect computers from security breaches via these vulnerabilities. Moreover, the task of maintaining security for these computer systems and/or networks has become increasingly burdensome and difficult.

[0003] Currently, organizations typically use vulnerability scanning software or managed security providers to test computers for security weaknesses. These tools generally provide detailed information on the vulnerabilities found in the computing environment, but provide limited means for correcting or resolving the detected vulnerabilities. In order for an

organization to remove identified vulnerabilities, it typically must expend a large amount of labor and resources to identify and/or create a remediation for each vulnerability then even more labor to install the vulnerability remediation on the affected computers. Often, this involves visiting each individual computer and manually applying the necessary remediation. In addition, once the remediation is applied, a user can easily remove it, or install additional software that invalidates the remediation, thereby wasting all of the effort expended in performing the remediation.

SUMMARY OF THE INVENTION

[0004] In accordance with the present invention, a method and system are presented which provide for a more automated and managed way to remediate security vulnerabilities on individual computers and computer networks. More particularly, a vulnerability resolution system is provided in which vulnerability information is aggregated, then used to construct, and subsequently update, vulnerability remediation signatures for download. The downloaded signatures may then be selectively used to address or resolve vulnerabilities on client machines having security vulnerabilities.

[0005] In one embodiment, a method for resolving vulnerabilities in a computer comprises aggregating vulnerability information on a plurality of computer vulnerabilities; constructing a remediation database of said plurality of computer vulnerabilities; constructing a remediation signature to address a computer vulnerability; and deploying said remediation signature to a client computer. The aggregating of vulnerability information comprises obtaining vulnerability information from at least one security intelligence agent, such as a database of information regarding known computer vulnerabilities or a scanning service which scans a client computer for vulnerabilities and records the vulnerability information. The remediation signature typically comprises a sequence of actions to address a corresponding vulnerability. The remediation signatures are generally associated with a corresponding computer vulnerability. A remediation profile may be constructed for a client computer to address vulnerabilities on that computer, where the profile comprises selected remediation signatures for the client computer corresponding to vulnerabilities on the client computer. The remediation signatures may be uploaded to a flash server for remote access or download by client computers or client servers. A managed remediation approach is also contemplated which would include wherein selective deployment of remediation signatures, selective resolution of vulnerabilities, scheduled scanning of client computers for vulnerabilities, scheduled deployment of remediation signatures, etc.

[0006] In another embodiment, a system for resolving computer vulnerabilities comprises a remediation server capable of coupling to a security intelligence agent having information about computer vulnerabilities in order to aggregate said vulnerability information into a remediation database. Various devices may be coupled to the remediation server to complete the system. For example, a signature module may be coupled to the remediation server to construct a remediation signature for each vulnerability. A flash server may be coupled to the signature module to provide remote access to said remediation signatures. A client server may also be included capable of coupling to said flash server to access said remediation signatures. A deployment module may be coupled to the client server capable of deploying said remediation signatures to a client computer coupled to said client server. The deployment module may also be capable of constructing a remediation profile for a client computer to address vulnerabilities on that computer, wherein the remediation profile typically comprises selected remediation signatures for the client computer corresponding to vulnerabilities on the client computer. An input module may also be coupled to the remediation server to handle the interfacing of the remediation server to a security intelligence agent having information about computer vulnerabilities. And a client module may be coupled to the client server to which handle the interfacing of the client server to the flash server to access said remediation signatures.

[0007] In another embodiment, computer-readable media tangibly embodying a program of instructions executable by a computer to perform a process for resolving vulnerabilities in a computer comprises aggregating vulnerability information on a plurality of computer vulnerabilities; constructing a remediation database of said plurality of computer vulnerabilities; constructing a remediation signature to address a computer vulnerability; and deploying said remediation signature to a client computer.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] Figure 1 is a block diagram illustrating an embodiment of a vulnerability resolution system in accordance with the present invention.

[0009] Figure 2 is a block diagram illustrating another embodiment of a vulnerability resolution system in accordance with the present invention.

[00010] Figure 3 is a flow chart illustrating an overview of an embodiment of a computer vulnerability remediation process in accordance with the present invention.

[00011] Figure 4 is a flow chart illustrating an embodiment of an aggregation and construction process for computer vulnerability remediation in accordance with the present invention.

[00012] Figure 5A and 5B are a flow chart illustrating an embodiment of a remediation management process for computer vulnerability remediation in accordance with the present invention.

DETAILED DESCRIPTION OF EMBODIMENTS

[00013] In this disclosure, numerous specific details are set forth to provide a sufficient understanding of the present invention. However, those skilled in the art will appreciate that the present invention may be practiced without such specific details. In other instances, well-known elements have been illustrated in schematic or block diagram form in order not to obscure the present invention in unnecessary detail. Additionally, some details have been omitted inasmuch as such details are not considered necessary to obtain a complete understanding of the present invention, and are considered to be within the understanding of persons of ordinary skill in the relevant art. It is further noted that all functions described herein may be performed in either hardware or software, or a combination thereof, unless indicated otherwise. Certain terms are used throughout the following description and claims to refer to particular system components. As one skilled in the art will appreciate, components may be referred to by different names. This document does not intend to distinguish between components that differ in name, but not function. In the following discussion and in the claims, the terms "including" and "comprising" are used in an open-ended fashion, and thus should be interpreted to mean "including, but not limited to...". Also, the term "couple" or "couples" is intended to mean either an indirect or direct electrical or communicative connection. Thus, if a first device couples to a second device, that connection may be through a direct connection, or through an indirect connection via other devices and connections. Finally, the terms "remediate" and "remediation" are used to refer generally to addressing or resolving vulnerabilities by reducing or alleviating the security risk presented by the subject vulnerability.

[00014] Figure 1 illustrates an embodiment of a vulnerability resolution system 10 in accordance with the present invention. As shown in Figure 1, the system 10 comprises a remediation server 12 coupled to a plurality of intelligence agents 14. The remediation server 12 is also coupled to an import module 15, a remediation database 16, and a signature module 18. In this embodiment, the import module 15, remediation database 16, and signature module 18 are incorporated in the remediation server 12. For instance, the import module 15, remediation database 16, and signature module 18 may be stored in memory on the remediation server 12. It is also contemplated, however, that the import module 15,

remediation database 16, and signature module 18 could be remotely coupled to the remediation server 12.

[00015] A flash server 20 is also coupled to the remediation server 12. A client server 22 is coupled to the flash server 20. A client module 23 and deployment module 24 are coupled to the client server 22. In this embodiment, the client module 23 and deployment module 24 are incorporated in the client server 22. For instance, the client module 23 and deployment module 24 may be stored in memory on the client server 22. It is also contemplated, however, that the client module 23 and deployment module 24 could be remotely coupled to the client server 22. And finally, a plurality of client computers 26 are coupled to the client server 22.

[00016] In the operation of the system 10, the remediation server 12 obtains information relating to computer security vulnerabilities from the intelligence agents 14. The import module 15 provides the necessary interface between the remediation server 12 and the various intelligence agents having such information. Examples of intelligence agents include: ISS Internet Scanner, QualysGuard, Nessus, Eeye, Harris, Retina, Microsoft's hfNetCheck, and others. The vulnerability information may come in many forms from these agents. Two such forms include 1) general information from security intelligence organizations relating to known security vulnerabilities, such as vulnerabilities in widespread software applications like Microsoft Windows; and 2) specific information from scanning services relating to specific vulnerabilities found during a security scan of a client's computer or computer system 26. The remediation server 12 aggregates the vulnerability information obtained, from whatever source, into a remediation database 16. While aggregating the information into the database 16, the remediation server 12 may manipulate the information in many ways. For example, the server 12 may strip unnecessary information out, may sort the information into related vulnerabilities or otherwise, may remove duplicate information, may identify or associate certain related vulnerabilities, etc.

[00017] In addition, the remediation server 12 uses a signature module 18 to generate remediation signatures for the vulnerabilities. Typically, a remediation signature is a list of actions taken to address or resolve a vulnerability. In this embodiment, the remediation signatures include the following types of remediation actions: service management, registry management, security permissions management, account management, policy management, audit management, file management, process management, as well as service pack, hot fix and patch installation. These types of remediation actions are generally known in the computer security industry.

[00018] A remediation signature may address one or more vulnerabilities. For clarity of explanation, however, it will be assumed that in this embodiment each remediation signature addresses a single vulnerability or type of vulnerability. In an embodiment of this system, the remediation signatures are generated as abstract objects which can be developed and implemented across multiple platforms without the need to change the underlying source code used in the remediation system. This allows for the creation of a remediation signature in the environment of the remediation system which can then be utilized in whatever system or environment the remediation system is operating. The process of constructing a remediation signature may be entirely automatic or it may involve some manual intervention, or a combination of both. In fact, some intelligence agents 14 may actually provide or suggest remediations along with the vulnerability information provided. Depending on the level of complexity of the vulnerability, a corresponding level of complexity may be required for the remediation signature. For example, some vendors provide "patches" or "fixes" or "updates" that address vulnerabilities in their hardware or software via their vendor website. A signature may therefore include direction to go to a vendor website and retrieve a patch or an update as one of the actions undertaken to remediate a computer's vulnerabilities. Given the potential complexity of the signatures, they may not always operate successfully as initially constructed. Accordingly, the signature module 18 or remediation server 12 may have the ability to test and approve the constructed signature in order to ensure that it successfully resolves the intended vulnerability and does not have any unintended deleterious effects.

[00019] Once a remediation signature has been constructed, in this embodiment of the system 10 the remediation signature is assigned or otherwise associated with the corresponding vulnerability in the remediation database 16. Accordingly, the remediation database 16 may include the vulnerability information and the corresponding remediation signatures for the vulnerabilities identified. Alternatively, it is contemplated that the signatures could be stored elsewhere and remotely associated via a pointer or otherwise to their corresponding vulnerabilities.

[00020] Remediation signatures and vulnerability information can be posted to the flash server 20 for dissemination. Typically, only after the remediation signature has been tested and approved is it released or uploaded to the flash server 20 for dissemination to clients seeking resolution of their computer vulnerabilities. A client server 22 can then download the desired information from the flash server 20. In this embodiment, a download is typically initiated by a user, such as an IT or computer security personnel. The client server 22 may

connect to the flash server 20 in many ways including the Internet or a direct dial-up connection. In this embodiment of the system, the client module 23 provides the necessary interface logic to download the information from the flash server 20. Typically, a client server 22 will periodically download information from the flash server 20 to check for updated vulnerability and remediation information. The client server 22 may also access vendor websites 21, via a global network such as the Internet or otherwise, to obtain additional patches or updates as needed for remediation. In this embodiment of the system 10, the client server 22 analyzes and interprets the signatures downloaded from the flash server 20. If a signature specifies a needed update or patch from a vendor website 21, the client server 22 will connect to the website and download the needed information making the patch or update available locally for remediation of any client computers 26 coupled to the client server 22.

[00021] In this embodiment, it is also contemplated that the client server 22 will keep a profile of the client computers 26 coupled thereto. The profile of the client computers 26 essentially records or logs the system information relating to the client computers 26. Primarily, the profile contains information regarding remediation performed on the client computer 26. It is contemplated, however, that the profile might also contain information regarding the formatting of the client computer 26, the software applications and versions running on the computer 26, etc., which might be helpful in managing security issues on the subject computer. By comparing the computer profiles with the vulnerability and remediation information downloaded from the flash server 20, the client server 22 can track what remediation may be required for each client computer 26. In addition, the client server 22 can manage the vulnerability resolution process for each client computer 26. For instance, the client server 22, or security or IT personnel via the server, could select which remediation signatures should be deployed to each client computer 26, or which vulnerabilities should or should not be addressed. In addition, vulnerability resolution can be managed by scheduling the various resolution events. For instance, when and how often the client computers 26 are scanned for vulnerabilities can be scheduled, as well as the timing of the deployment of the remediation signatures to address those vulnerabilities.

[00022] By managing the vulnerability resolution, the remediation of vulnerabilities can be more reliably and more cost effectively addressed. In particular, the remediation can occur in off hours to minimize impact on the productivity of the client computers 26. The remediation can be selectively implemented. The remediation can be tracked and logged so that remediations are not accidentally overwritten or undone. And, the remediation can be

accomplished automatically from the client server 22 as opposed to having to perform or install the remediation manually on each client computer, a virtually impossible task for some large-scale companies.

[00023] Figure 2 is a block diagram providing another illustration of an embodiment of a vulnerability resolution system 30 in accordance with the present invention. More particularly, Figure 2 provides another way to visualize the architecture of a vulnerability system in accordance with the present invention. As shown in Figure 2, the architecture of this embodiment of the vulnerability system 30 generally comprises an aggregation section 31 and a remediation section 32. The aggregation section 31 of the architecture is essentially responsible for obtaining and aggregating the computer security vulnerability information while the remediation section 32 is essentially responsible for constructing remediation signatures for the identified vulnerabilities and deploying those remediations to client computers in a managed and automated manner.

[00024] As shown in Figure 2, the aggregation section 31 of the system architecture 30 comprises intelligence agents 34, an import API or interface 36, and an administrator 38. The import API 36 provides an interface to the intelligence agents 34. As discussed in reference to Figure 1 above, the intelligence agents 34 provide information regarding computer security vulnerabilities. As noted, these intelligence agents 34 may include automated vulnerability assessment tools, security intelligence services, manufacturers of computer hardware or software, etc. The administrator 38 obtains this vulnerability information from the intelligence agents 34 via the import API 36. The import API 36 typically includes several interfaces or import wizards as required to allow importation of vulnerability assessment data from the variety of intelligence agents available. Generally, the intelligence agents 34 provide information specifying the necessary interface. Once retrieved, the vulnerability information may be aggregated, sorted, selected or otherwise managed via the administrator 38.

[00025] The remediation section 32 of the system architecture 30 ultimately uses the vulnerability information retrieved by the aggregation section 31 to remediate vulnerabilities on client computers 40. The client computers 40 are shown coupled to a client server 42. The client server 42 allows for automated and managed deployment of the remediation signatures to the client computers 40. The architecture of the remediation section 32 illustrates that the vulnerability information from the aggregation section 31 is conveyed to the client server 42 and client computers 40 via the remediation bus 44, remediation signature 46, and remediation profile 48. As discussed above, the remediation signature 46 is

essentially a group of actions which can be taken to address or resolve a vulnerability. The signature may be provided by the intelligence agents 34 with the vulnerability information or, more typically, it may need to be constructed in response to the vulnerability information received. The construction may include some automated creation and/or some manual creation of the appropriate actions to be taken to address the subject vulnerability. Also as discussed, the remediation profile 48 contemplates a record or log of system information relating to the client computers 40 or client servers 42. For instance, the profile may contain information regarding the formatting of the client computers 40 or server 42, the software applications and versions running on the computers 40 or servers 42, the remediation signatures already implemented on the computers 40 and servers 42, the remediation history of the computers 40, etc. By comparing the computer profiles with the vulnerability and remediation information obtained, what remediation may be required for each computer 40 or server 42 can be tracked. Figure 2 also illustrates that the remediation types or groups 50 in this embodiment include configuration management, backdoor management, service management, account management, and patch management. The available remediation groups are coupled to the remediation bus 44.

[00026] Figure 3 is a flow chart illustrating an overview of an embodiment of a computer vulnerability remediation process in accordance with the present invention. The remediation process 60 begins with vulnerability assessment in box 61. Vulnerability assessment comprises using automated assessment tools and audit processes, intelligence agents, to verify the existence of known vulnerabilities on a given computer or computer network. This assessment process may also include device discovery; that is, the mapping of network and subnetwork components to be assessed and identifying the devices that will be targeted for vulnerability assessment. In box 62, the vulnerability information is imported or aggregated in the system, typically in a remediation database, and remediation signatures can be constructed to address the identified vulnerabilities. As noted, the remediation signatures are typically associated with the corresponding vulnerabilities in the remediation database. The vulnerability information is then reviewed in box 63. The review process typically includes analyzing the vulnerability information to prioritize and identify vulnerabilities for remediation, as well as acceptable risks (i.e., where no remediation is required). As indicated in box 64, the remediation can then be scheduled to occur when, where, and how desired. This allows the remediation to occur in off-peak times to reduce interference with normal computer operations, on only the identified target computers, and in the manner desired. In box 65, the remediation signatures are approved for dissemination to the client's target

computers. This contemplates that remediation signatures can be selectively deployed. In addition, signatures designed to address the vulnerabilities identified may be tested and revised before approving the signatures for deployment. Once approved, the remediation signatures and vulnerability information are distributed to the system clients in box 66 for use on the client's computers. Then, remediation can occur as scheduled in box 67. Finally, the remediation undertaken can be reviewed to ensure the remediation was completed successfully via status reports or otherwise. In addition, remediation events may be logged or otherwise recorded to preserve the remediation information. Such information may be included in profiles for the client computers. As noted, such profiles may include information about the target devices such as system configuration, software, and prior remediation actions or a remediation history. Having such information allows for managed remediation of the client computers in the future. Overall then, the embodiment of the remediation process of Figure 3 presents vulnerability assessment, vulnerability remediation, and vulnerability management as contemplated by the present invention.

[00027] Figure 4 is a flow chart illustrating an embodiment of an aggregation and construction process for computer vulnerability remediation in accordance with the present invention. Essentially, the aggregation and construction process 70 can be viewed as a subprocess of the overall remediation process. The process 70 begins in box 71 with the gathering of vulnerability information from intelligence agents. As previously noted, these intelligence agents include automated vulnerability assessment tools, security intelligence services, manufacturers of computer hardware or software, etc. The vulnerability information retrieved from the intelligence agents is then aggregated in a remediation database as indicated in box 72. In box 73, the vulnerability information is then reviewed and analyzed. This may include sorting the information into related vulnerabilities or otherwise, categorizing or identifying certain related vulnerabilities, prioritizing vulnerabilities, etc. As indicated in box 74, vulnerabilities are identified for creation of remediation signatures. A remediation signature resolves or addresses a vulnerability or type of vulnerability. A remediation signature is then constructed in box 75. As noted, a remediation signature is a group of actions which addresses or resolves the subject vulnerability; for instance, modifying registry settings, changing security permissions, installing patches, etc. The creation of a remediation signature may be completely automated or may include some manual input as well. In box 76, the remediation signature is tested to see if it effectively resolves or addresses the target vulnerability. If not, the process returns to box 75 and another remediation signature is constructed, then retested in box 76. Once an effective

signature has been constructed, the process continues to box 77. In box 77, selected signatures may be approved for distribution to clients. Approved signatures are then uploaded to a flash server making them available for download by clients in box 78. In this way, new and updated remediation signatures which address or resolve identified vulnerabilities are made available for download by clients.

[00028] Figures 5A and 5B are a flow chart illustrating an embodiment of a remediation management process for computer vulnerability remediation in accordance with the present invention. Essentially, the aggregation and construction process 70 can be viewed as a subprocess of the overall remediation process. This embodiment of the remediation management process 80 is typically a software application installed on a client server which is coupled to a plurality of target client computers which may require remediation of security vulnerabilities. Accordingly, the process 80 begins in box 81 by launching the application. In box 82, available remediation signatures and vulnerability information are downloaded, typically from a flash server. In box 83, vulnerability assessment data is imported. Typically, this vulnerability assessment data comes from scanning tools which have scanned or analyzed the target computers for which remediation is being considered. The vulnerability assessment data includes information regarding the security vulnerabilities found on the target computers or devices. Based on the vulnerabilities identified on the target computers, the vulnerabilities are then mapped to remediation signatures in box 84. In this embodiment, mapping of the identified vulnerabilities to corresponding remediation signatures occurs by referencing the remediation database information downloaded from the flash server. It is contemplated, however, that this information may have been previously downloaded, remotely accessed, or presently downloaded to make the necessary correlation between vulnerabilities and available signatures. A remediation profile is then generated for each target computer in box 85. As noted, the profile typically includes information regarding the vulnerabilities identified on the target client computer as well as the corresponding signatures to address those vulnerabilities. In box 86, the client user, typically an IT person or other computer security personnel, is given the opportunity to select which vulnerabilities should be remediated. Generally, the selection is made by reviewing the information regarding vulnerabilities, proposed signatures, and profiles. The selection and review may be made for each computer or by vulnerability. For example, a particular computer could be selected not to receive any remediation, perhaps because the computer does not pose a significant security risk, the vulnerabilities on the computer are not significant, the processes running on the computer cannot be interrupted for remediation, etc.

Alternatively, a particular vulnerability could be deselected for all target client computers, such that the vulnerability would not be remediated on any of the target computers, perhaps because the vulnerability dose not pose a sufficient security risk, the remediation signature is deemed too risky, etc. Once the user has selectively managed which vulnerabilities will be remediated, the user can then select which computers will be approved to receive remediation in box 87. In box 88, the proposed remediation is analyzed to determine which remediation signatures will be required. In box 89, the target client computers that are to receive remediation are notified that a remediation is to occur. In this embodiment, the notification essentially comprises a message passed to a local remediation application installed on each client computer. Included in the remediation notification may be when the remediation is scheduled to occur. For instance, the remediation can be scheduled to occur at the instance of a particular event, such as a user logging off the machine, logging in, or any other action. In addition, the remediation may be scheduled to occur at a particular time. Thus, using the target client computer's local clock the remediation can be initiated at the scheduled time. Or alternatively, the remediation could occur as soon as the notification is received at the target client computer. Regardless of the triggering event, when the trigger is met the local remediation is launched in box 90.

[00029] The process 80 continues in Figure 5B. Once the remediation is launched, the remediation profile for the client computer is then downloaded in box 91. Typically, the profile is downloaded from the client server on which the client remediation management process application is running, i.e., the server that sent the notification of the pending remediation initially. The profile is then interpreted and the remediation signatures and actions specified in the profile are executed as indicated in box 92. As noted in box 93, during remediation the status of the remediation may be reported to the client server and monitored. In addition, the remediation steps may be prioritized and analyzed to ensure the most efficient sequence of execution as indicated in box 94. As noted in box 95, a reboot may need to be performed for some of the remediation actions to take effect. Completion of the remediation on the target client computer is then logged to the client server in box 96. Once remediation is completed, box 97 indicates that reports are generated indicative of the effect of the remediation. Whether the remediation was successful or not is determined in box 98. If the remediation is not deemed successful, either because it did not resolve the identified vulnerabilities as evidenced by an additional security scan of the client computer, or because the remediation actions had unintended deleterious effects, etc., then the remediation can be rolled back or undone and the remediation process can be repeated as

indicated in box 99. If the remediation is deemed successful, i.e., vulnerabilities resolved and no deleterious effects for example, then the process ends in box 100. In this manner, the new and updated remediation signatures made available to address or resolve identified vulnerabilities can be downloaded and used in an automated and managed remediation deployment to target client computers.

[00030] While the present invention has been illustrated and described in terms of particular apparatus and methods of use, it is apparent that equivalent parts may be substituted for those shown and other changes can be made within the scope of the present invention as defined by the appended claims.

[00031] The particular embodiments disclosed herein are illustrative only, as the invention may be modified and practiced in different but equivalent manners apparent to those skilled in the art having the benefit of the teachings herein. Furthermore, no limitations are intended to the details of construction or design herein shown, other than as described in the claims below. It is therefore evident that the particular embodiments disclosed above may be altered or modified and all such variations are considered within the scope and spirit of the invention. Accordingly, the protection sought herein is as set forth in the claims below.

CLAIMS:

What is claimed is:

1. A method for resolving vulnerabilities in a computer, comprising:

aggregating vulnerability information on a plurality of computer vulnerabilities; and

constructing a remediation database of said plurality of computer vulnerabilities.

2. The method of claim 1 further comprising constructing a remediation signature to address a computer vulnerability.

3. The method of claim 2 further comprising deploying said remediation signature to a client computer.

4. The method of claim 1 wherein said aggregating of vulnerability information comprises obtaining vulnerability information from at least one security intelligence agent.

5. The method of claim 4 wherein said security intelligence agent comprises a database of information regarding known computer vulnerabilities.

6. The method of claim 4 wherein said security intelligence agent comprises a scanning service which scans a client computer for vulnerabilities and records the vulnerability information.

7. The method of claim 2 wherein a remediation signature comprises a sequence of actions to address a corresponding vulnerability.

8. The method of claim 2 wherein said constructing a remediation database further comprises associating each remediation signature to a corresponding computer vulnerability.

9. The method of claim 1 wherein said constructing a remediation database further comprises constructing, testing and approving a remediation signature corresponding to a vulnerability.

10. The method of claim 3 wherein said deploying said remediation signatures comprises providing remote access to said remediation signatures.

11. The method of claim 3 wherein said deploying said remediation signatures comprises constructing a remediation profile for a client computer to address vulnerabilities on that computer.

12. The method of claim 3 wherein said remediation profile comprises selected remediation signatures for the client computer corresponding to vulnerabilities on the client computer.

13. The method of claim 10 wherein said deploying said remediation signatures further comprises uploading approved remediation signatures to a flash server for remote access by client computers or client servers.

14. The method of claim 13 wherein said deploying said remediation signatures further comprises downloading remediation signatures from said flash server to a client server.

15. The method of claim 3 wherein said deploying said remediation signatures comprises managing vulnerability resolution.

16. The method of claim 15 wherein said managing vulnerability resolution comprises selective deployment of remediation signatures.

17. The method of claim 15 wherein said managing vulnerability resolution comprises selective resolution of vulnerabilities.

18. The method of claim 15 wherein said managing vulnerability resolution comprises scheduled scanning of client computers for vulnerabilities.

19. The method of claim 15 wherein said managing vulnerability resolution comprises scheduled deployment of remediation signatures.

20. A system for resolving computer vulnerabilities; comprising:

a remediation server capable of coupling to a security intelligence agent having information about computer vulnerabilities in order to aggregate said vulnerability information into a remediation database.

21. The system of claim 20 further comprising a signature module coupled to said remediation server to construct a remediation signature for each vulnerability.

22. The system of claim 21 further comprising a flash server coupled to said signature module to provide remote access to said remediation signatures.

23. The system of claim 22 further comprising a client server capable of coupling to said flash server to access said remediation signatures.

24. The system of claim 23 further comprising a deployment module coupled to said client server capable of deploying said remediation signatures to a client computer coupled to said client server.

25. The system of claim 24 wherein said deployment module is capable of constructing a remediation profile for a client computer to address vulnerabilities on that computer.

26. The system of claim 25 wherein said remediation profile comprises selected remediation signatures for the client computer corresponding to vulnerabilities on the client computer.

27. The system of claim 20 wherein said security intelligence agent comprises a database of information regarding known computer vulnerabilities.

28. The system of claim 20 wherein said security intelligence agent comprises a scanning service which scans a client computer for vulnerabilities and records the vulnerability information.

29. The system of claim 20 wherein said remediation server assigns a remediation signature to each vulnerability.

30. The system of claim 21 wherein said signature module is capable of constructing, testing and approving a remediation signature.

31. The system of claim 22 wherein said flash server provides access to approved remediation signatures.

32. The system of claim 22 wherein said remediation signatures are uploaded to said flash server.

33. The system of claim 23 wherein said client server downloads said remediating signatures from said flash server.

34. The system of claim 24 wherein said deployment module allows managed vulnerability resolution.

35. The system of claim 34 wherein said managed vulnerability resolution comprises selective deployment of remediation signatures.

36 The system of claim 34 wherein said managed vulnerability resolution comprises selective resolution of vulnerabilities.

37. The system of claim 34 wherein said managed vulnerability resolution comprises scheduled scanning of client computers for vulnerabilities.

38. The system of claim 34 wherein said managed vulnerability resolution comprises scheduled deployment of remediation signatures.

39. The system of claim 24 wherein said deployment module constructs a remediation profile for each client computer.

40. The system of claim 39 wherein said remediation profile comprises remediation signatures to resolve vulnerabilities on said client computer.

41. The system of claim 39 wherein said remediation signatures can be selectively included in said remediation profile.

42. The system of claim 21 wherein said remediation signature comprises a sequence of actions to address a corresponding vulnerability.

43. The system of claim 20 further comprising an input module coupled to said remediation server which handles the interfacing of the remediation server to a security intelligence agent having information about computer vulnerabilities.

44. The system of claim 23 further comprising a client module coupled to said client server which handles the interfacing of the client server to the flash server to access said remediation signatures.

45. Computer-readable media tangibly embodying a program of instructions executable by a computer to perform a process for resolving vulnerabilities in a computer, comprising:

aggregating vulnerability information on a plurality of computer vulnerabilities; and

constructing a remediation database of said plurality of computer vulnerabilities.

46. The media of claim 45 wherein the process further comprises constructing a remediation signature to address a computer vulnerability.

47. The media of claim 45 wherein the process further comprises deploying said remediation signature to a client computer.

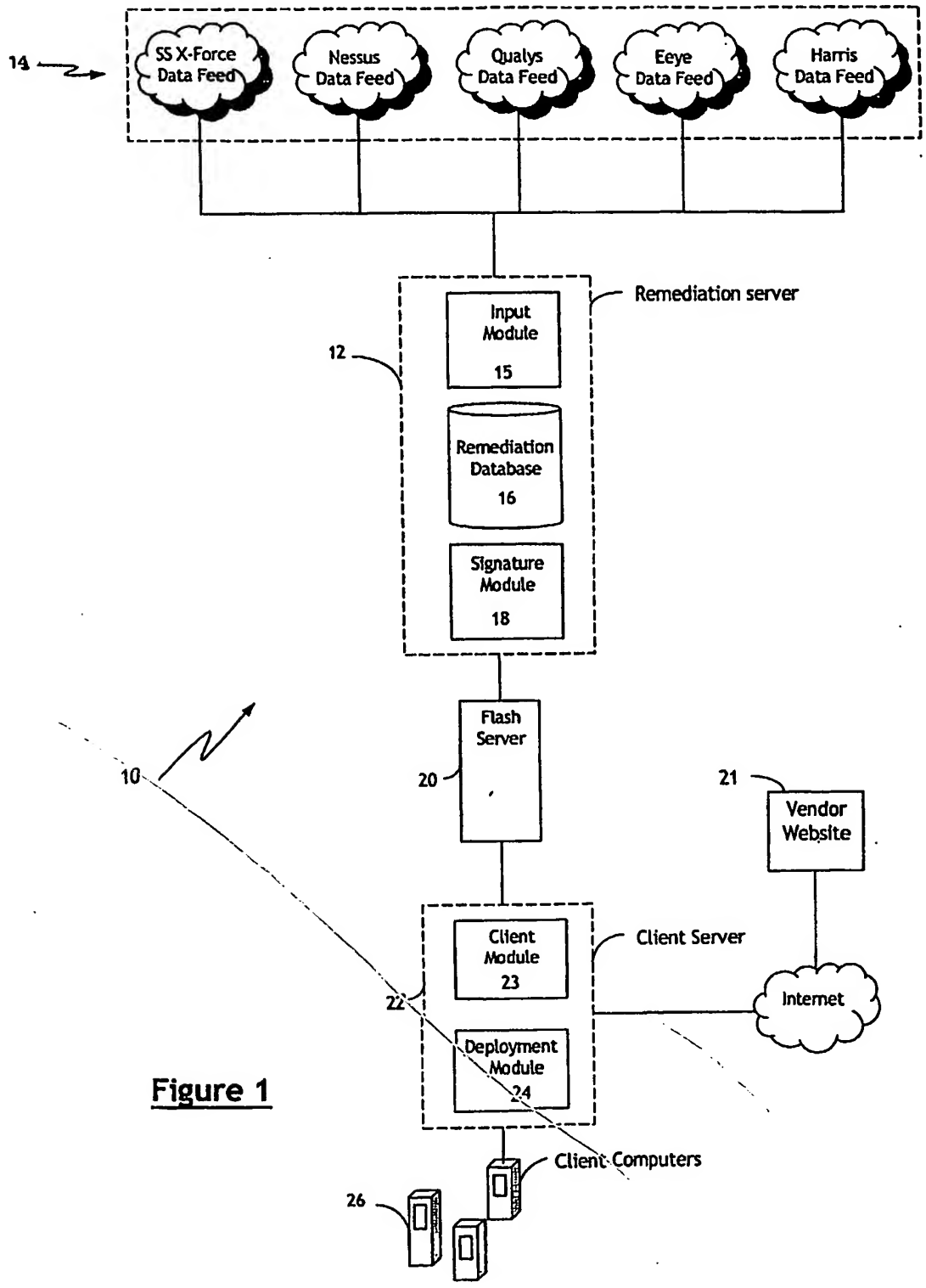

14
SS X-Force Data Feed
Nessus Data Feed
Qualys Data Feed
Eeye Data Feed
Harris Data Feed
Remediation server
12
Input Module 15
Remediation Database 16
Signature Module 18
Flash Server
20
10
21
Vendor Website
Client Module 23
Client Server
22
Internet
Deployment Module 24
Client Computers
26

Figure 1

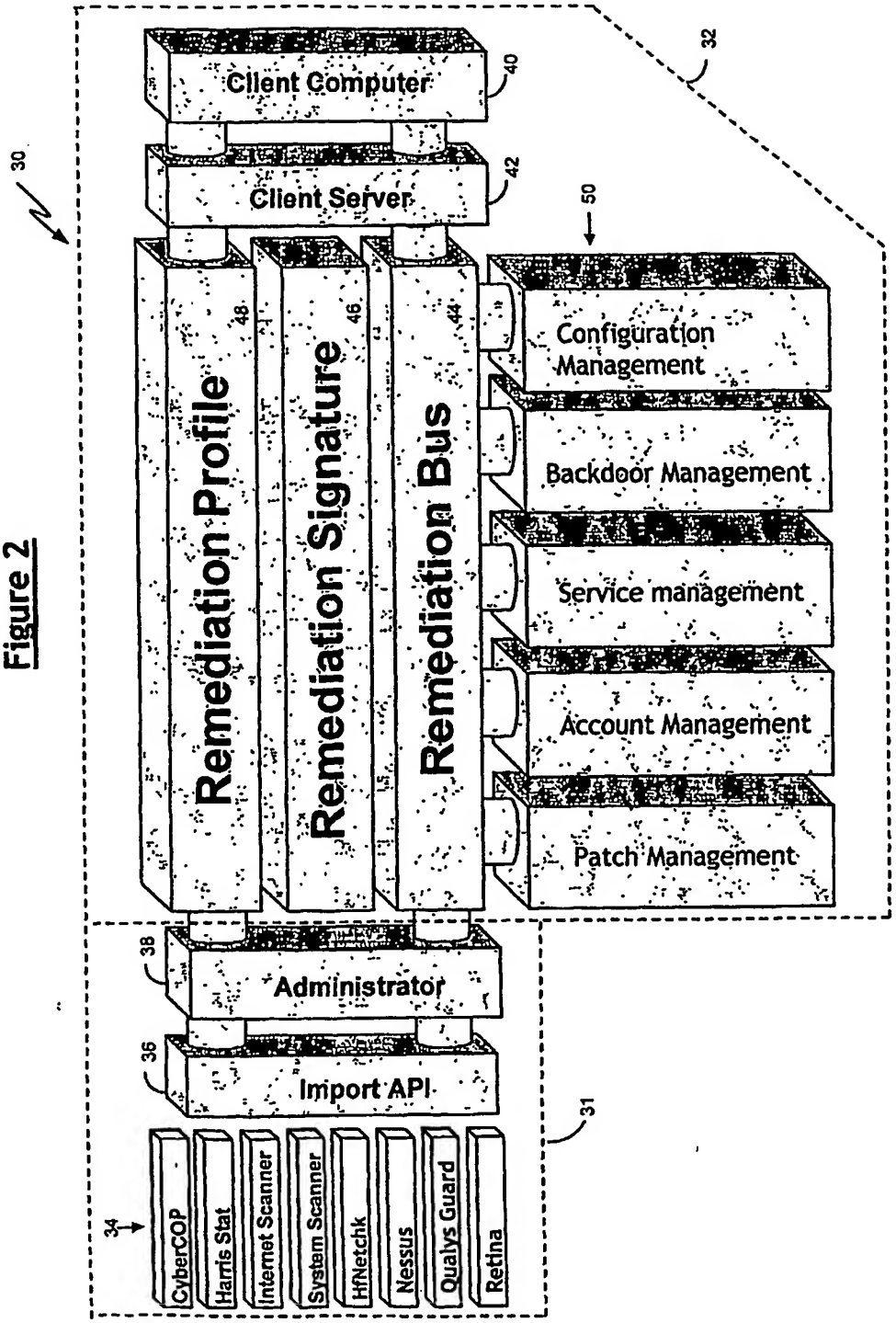

30
32
Client Computer
40
Client Server
42
50
Remediation Profile
48
Remediation Signature
46
Remediation Bus
44
Configuration Management
Backdoor Management
Service management
Account Management
Patch Management
38
Administrator
36
Import API
31
34
CyberCOP
Harris Stat
Internet Scanner
System Scanner
HFNetchk
Nessus
Qualys Guard
Retina

Figure 2

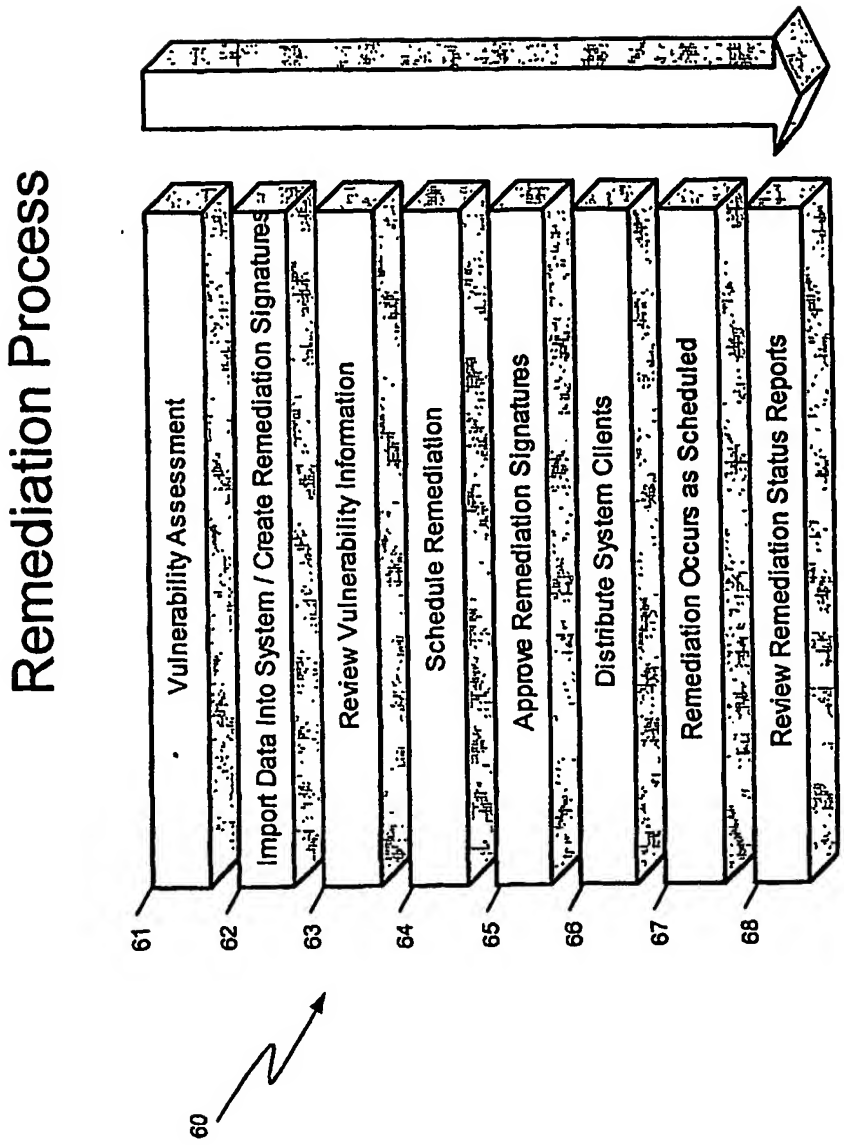

Remediation Process
Vulnerability Assessment
Import Data Into System / Create Remediation Signatures
Review Vulnerability Infomation
Schedule Remediation
Approve Remediation Signatures
Distribute System Clients
Remediation Occurs as Scheduled
Review Remediation Status Reports
61
62
63
64
65
66
67
68
60

Figure 3

FIGURE 4

Aggregation and Construction Process

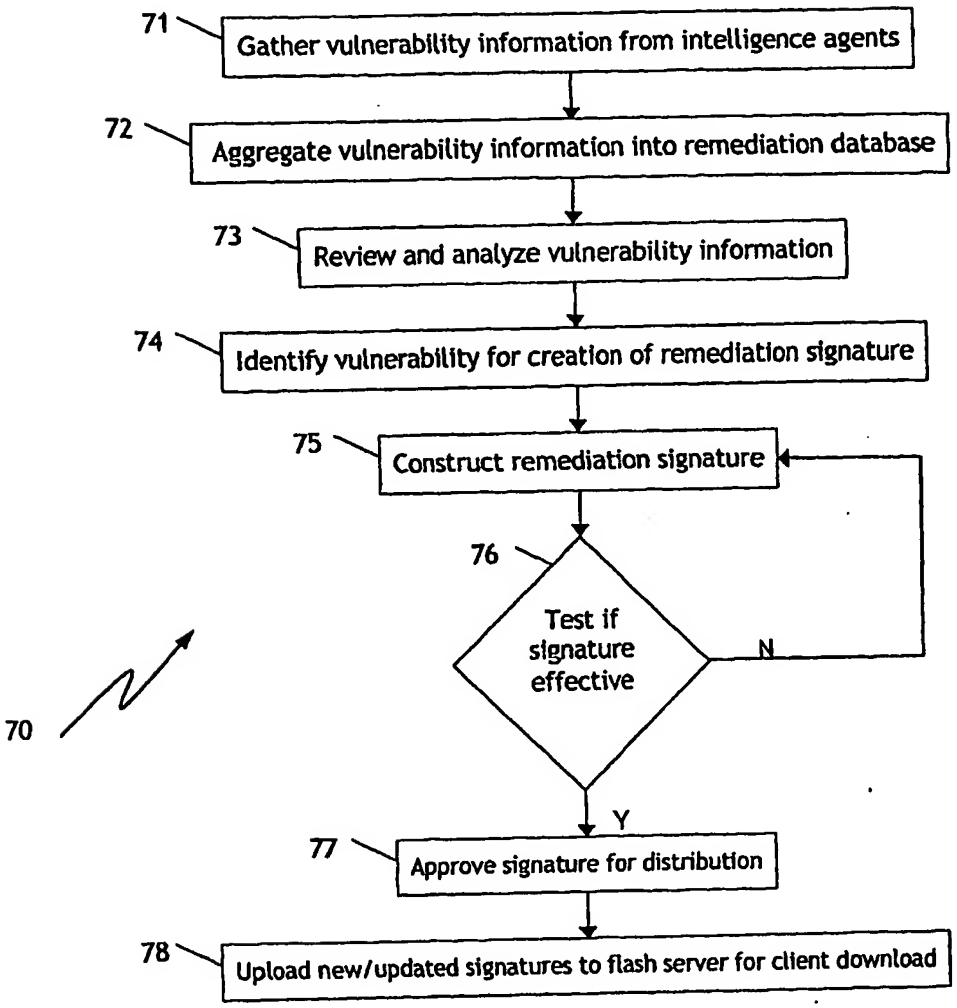


FIGURE 5A

Remediation Management Process

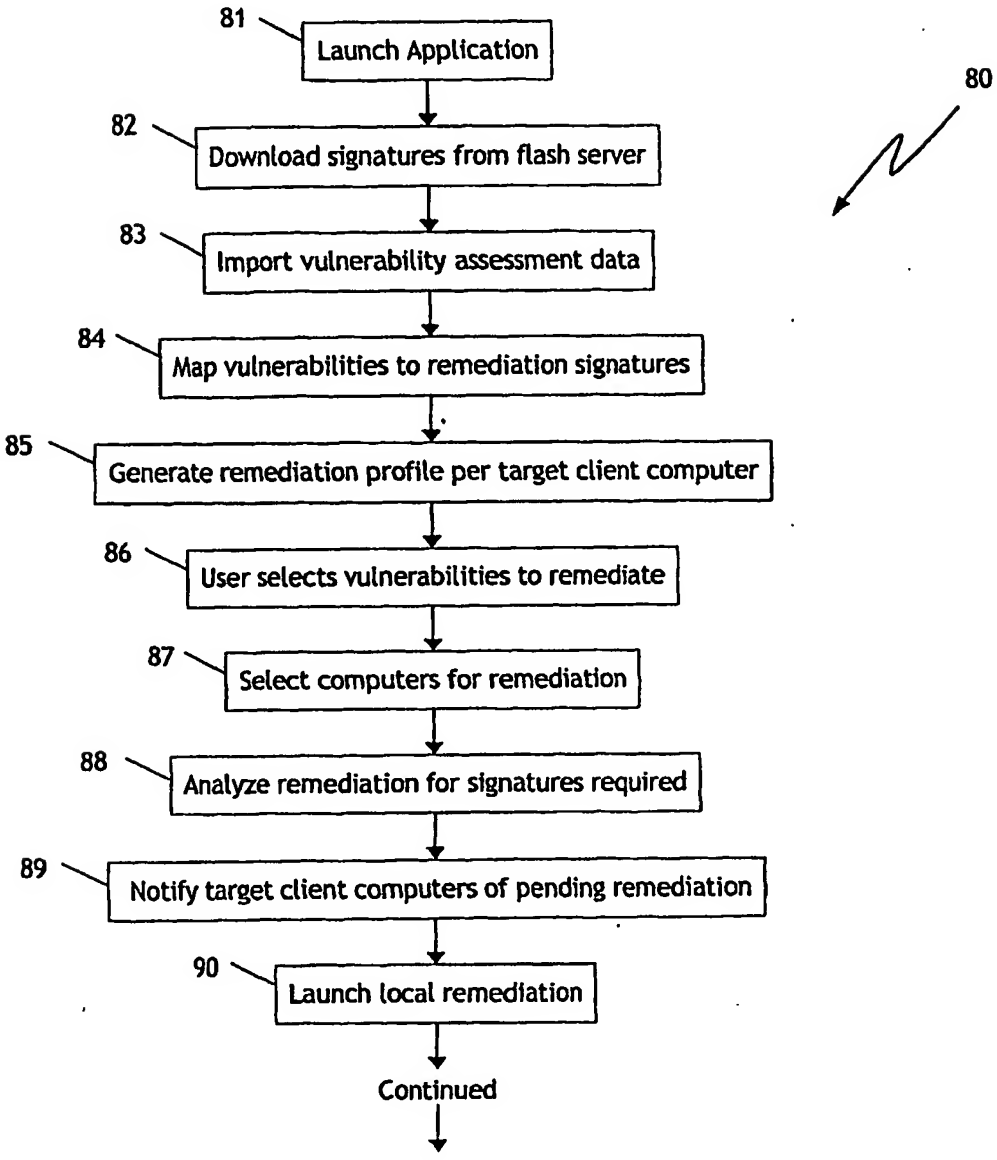
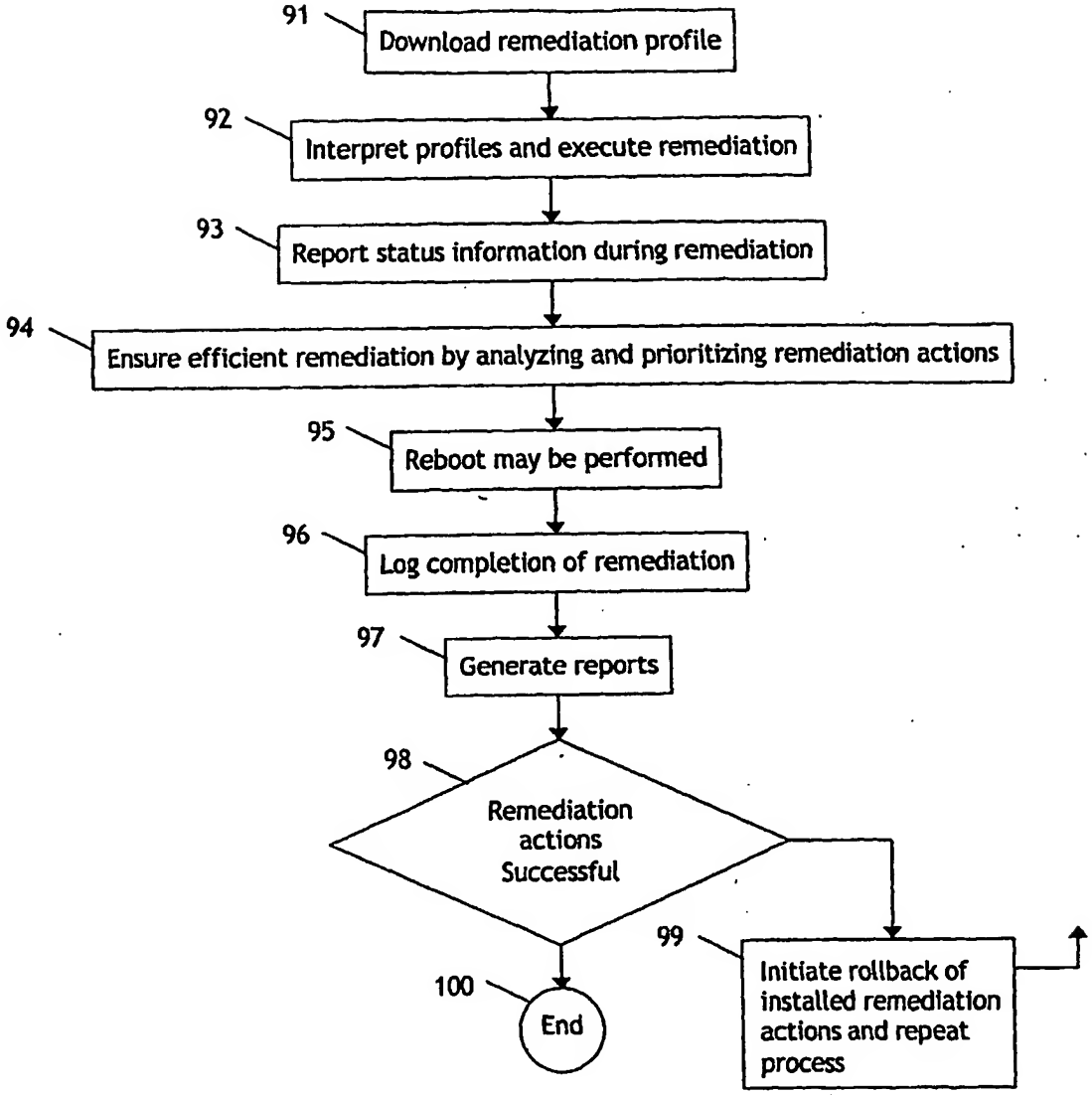


FIGURE 5B

Remediation Management Process



INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/41819

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 12/14; H04L 9/00
US CL : 713/200, 201; 709/224

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/200, 201; 709/224

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WEST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,298,445 A (SHOSTACK et al) 02 October 2001 (02.10.2001), column 3, lines 7-34 and column 3, line 66 to column 14, line 29.	1-47

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
03 March 2003 (03.03.2003)

Date of mailing of the international search report
28 MAR 2003

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703)305-3230

Authorized officer
Matthew B Smithers
Telephone No. (703) 305-3900

Form PCT/ISA/210 (second sheet) (July 1998)